

Generalized self-testing and the security of the 6-state protocol

Matthew McKague¹ and Michele Mosca^{1,2}

¹ Institute for Quantum Computing and Department of Combinatorics, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada

² Perimeter Institute for Theoretical Physics, 31 Caroline Street North, Waterloo, ON, N2L 2Y5, Canada

Abstract. Self-tested quantum information processing provides a means for doing useful information processing with untrusted quantum apparatus. Previous work was limited to performing computations and protocols in real Hilbert spaces, which is not a serious obstacle if one is only interested in final measurement statistics being correct (for example, getting the correct factors of a large number after running Shor’s factoring algorithm). This limitation was shown by McKague et al. to be fundamental, since there is no way to experimentally distinguish any quantum experiment from a special simulation using states and operators with only real coefficients.

In this paper, we show that one can still do a meaningful self-test of quantum apparatus with complex amplitudes. In particular, we define a family of simulations of quantum experiments, based on complex conjugation, with two interesting properties. First, we are able to define a self-test which may be passed only by states and operators that are equivalent to simulations within the family. This extends work of Mayers and Yao and Magniez et al. in self-testing of quantum apparatus, and includes a complex measurement. Second, any of the simulations in the family may be used to implement a secure 6-state QKD protocol, which was previously not known to be implementable in a self-tested framework.

1 Introduction

In [MY04], [MY98], Mayers and Yao introduced the concept of self-testing quantum apparatus with a test for EPR sources and a select set of measurements. In a parallel development, van Dam et al. [vMMS00] introduced the notion of self-testers for quantum circuits in the case where the dimension of the Hilbert space is known. These results were then combined and improved upon by Magniez et al. in [MMMO06], who give a construction for self-testable circuits without knowledge of the dimension of the Hilbert space.

The Mayers-Yao test, and the test of Magniez et al., only allowed for the testing of states and operators that are equivalent to states and operators in a real Hilbert space. McKague et al. [MMG09] showed that in such settings with untrusted apparatus, one cannot experimentally distinguish a quantum system with states and evolution involving complex amplitudes from a special simulation using only real amplitudes. In addition to the implications for self-testing untrusted quantum apparatus, this also resolved an open question posed by Gisin [Gis07] related to the violation of Bell inequalities. It is important to note that the real simulation does not preserve inner product relationships from the system it is simulating. At first glance, this suggests that the well-known 6-state protocol [BBBW84], [Bru98] might not be secure in a setting with untrusted apparatus, since the simulated versions of the six quantum states could be more distinguishable than the proofs of security assume, and an adversary could exploit this additional distinguishability and compromise security.

In fact, it is easy to describe such an insecure implementation of the 6-state protocol with untrusted apparatus, however even an implementation of standard BB84 quantum key establishment with untrusted apparatus is insecure if proper measures are not taken in order to rule out “side-channel” attacks. We show that with comparable precautions as those proposed by Mayers and Yao the 6-state protocol remains secure.

This paper starts by describing a general family of simulations that will reproduce the same statistics as any given “reference” experiment, and are thus experimentally indistinguishable from

said experiment. We show how the real Hilbert space simulation given in [MMG09] is equivalent to a special case of this family of simulations. The fact that these simulations work is not very surprising: they are essentially mixtures of the reference experiment, or the complex conjugate of the reference experiment. Thus, we have a more general collection of experiments that are experimentally indistinguishable in a self-testing framework. What is particularly remarkable is that we are able to describe, in section 4.1, a family of self-tests which can only be passed by simulations from the general family we describe (up to equivalence, as defined below). This is summarized in Theorem 2.

The self-tests allow us to put a physical experiment in a general collection of experiments, and we are then able to show that the 6-state protocol is secure for all the experiments within this collection. This shows that it is possible to define a secure 6-state protocol within the self-testing framework.

In section 3, we prepare for the proof of Theorem 2, by discussing the Mayers-Yao self-tested source result given in Theorem 1, a new proof of which is given in appendix C. This new proof is shorter and simpler, and more easily extended to prove our more general result.

Then, in section 4.1, we describe a new self-test for an EPR source and local measurement apparatus that will uniquely characterize the general equivalence class associated with this quantum state and measurement operators.

In section 5, we discuss the cryptographic implications, and why a properly self-tested 6-state protocol is still secure.

Lastly, in section 6, we discuss some open problems and future directions, including the robustness of the generalized self-tests.

2 Simulations

In this section we extend the work of McKague et al. in [MMG09]. There the authors gave a construction that allowed the outcomes of any experiment (the *reference* experiment) to be duplicated (*simulated*) by another experiment (the *simulation*) which is described entirely using real numbers. That is to say, all the states, measurement operators, unitaries, Kraus operators, and Hamiltonians are given as vectors and matrices over the real numbers. Of particular interest here is the fact that the simulation is, in general, not equivalent to the reference experiment according to definition 1 below.

In this section we give a construction for a wider family of simulations. The different simulations in the family are, in general, not equivalent to either the reference experiment nor each other. We will be most interested in states and measurements, but, as with the real simulation in [MMG09], it is also possible to simulate discrete and continuous time evolution.

The simulations rely on the simple observation that transforming an experiment by complex conjugation does not alter the statistics it generates. We could also take a classical mixture of the reference experiment and its complex conjugation, flipping a coin (or controlling on a qubit) beforehand to decide which one to perform. In the remainder of this section we fill in some details about the simulations defined by these mixtures.

2.1 States and measurements

Consider a reference state³ $|\psi\rangle$ measured according to a reference POVM $\{P_k\}$. We may duplicate the statistics of this experiment using the complex conjugate state $|\psi^*\rangle$ and POVM $\{P_k^*\}$. In

³ We may consider mixed states as well, but it is not necessary for our discussion.

addition, we could do some combination of the two; we may add an additional qubit register which records which of the two experiments to perform: $|0\rangle$ for the reference experiment, and $|1\rangle$ for the complex conjugate. This qubit may be in any state, and not necessarily pure. We then arrive at a new state

$$\rho' = a |0\rangle\langle 0| \otimes |\psi\rangle\langle \psi| + (1-a) |1\rangle\langle 1| \otimes |\psi^*\rangle\langle \psi^*| + c |0\rangle\langle 1| \otimes |\psi\rangle\langle \psi^*| + c^* |1\rangle\langle 0| \otimes |\psi^*\rangle\langle \psi| \quad (1)$$

with $a \geq 0$ and $|c| \leq \sqrt{a(1-a)}$. The important feature is that when we project onto $|0\rangle\langle 0|$ or $|1\rangle\langle 1|$ we get either $|\psi\rangle$ or $|\psi^*\rangle$, respectively. For the measurement, we form the POVM

$$\{|0\rangle\langle 0| \otimes P_k + |1\rangle\langle 1| \otimes P_k^*\}. \quad (2)$$

This POVM measurement is equivalent to measuring the added qubit, collapsing the state into either $|\psi\rangle$ or $|\psi^*\rangle$ and then measuring either $\{P_k\}$ or $\{P_k^*\}$ as appropriate; thus the statistics of the experiment are preserved.

Different simulations are arrived at by choosing different values of a and c . If $a = 1$ and $c = 0$ then we obtain the reference experiment. For $a = 0$ and $c = 0$ we obtain the complex conjugate. Another interesting case is when $a = c = \frac{1}{2}$, in which case we obtain (up to a local change of bases) the real simulation of [MMG09] as shown in appendix B.

2.2 Operators

Although it will not be necessary for our discussion, it is possible to simulate a reference experiment which includes evolution, according to a unitary, completely-positive map, or Hamiltonian. The details are discussed in appendix A.

2.3 Non-local computations

For multi-party experiments, such as the Mayers-Yao test, we would need the simulation to be performed in a local fashion with the measurements operating on local systems only. As defined above this not the case, but it is easy to modify the operators to make it so. We simply add an extra qubit for each party and record in each qubit whether to perform the reference experiment or the complex conjugate. We arrive at states analogous to that in equation 1, but with $|0\rangle$ and $|1\rangle$ replaced with logical states $|\bar{0}\rangle = |00\dots 0\rangle$, $|\bar{1}\rangle = |11\dots 1\rangle$ defined on the extra qubits held by the various parties. Finally, each party conditions their operations on their local copy of the qubit, applying either the reference operation or the complex conjugate.

3 Mayers-Yao self-test

The goal of the Mayers-Yao test is to compare two experiments. The first experiment is the *reference* experiment, which is the experiment we wish to implement. It is a blueprint, or gold standard, against which we compare the other experiment, the physical experiment, which is the experiment that is actually performed. Within the physical experiment we consider the entire physical apparatus, including the environment, so that we obtain a pure state on a Hilbert space of unknown dimension (however, we will limit ourselves to finite dimensions.) The reference and physical experiments consist of reference and physical states, operations, and measurements. The two experiments are compared through the statistics that they generate.

3.1 Equivalence

The proof considers a particular reference experiment, as described in section 3.2. This experiment is defined on a pair of qubits, so we will limit our discussion to such systems. As well, we consider only pure states - the physical system is unlimited (but finite) in size, so we may include the environment to obtain a pure state. The conclusion of Mayers and Yao is that if the statistics of a physical experiment agree with that of the reference experiment, then the physical experiment is equivalent to the reference experiment, under a particular notion of equivalence.

When defining a notion of equivalence in this setting we must first consider how we might change the reference experiment in a way that preserves the statistics of the outcomes. Any such change is invisible from the perspective of the statistics and hence we cannot rule them out. Here is a list of such changes:

1. Local changes of basis
2. Adding ancillae to physical systems, prepared in any joint state (the measurement does not act on them)
3. Changing the action of the observables outside the support of the state
4. Locally embedding the state and operators in a larger (or smaller) Hilbert space.

In order to accommodate these various changes we define equivalence as follows.

Definition 1. *A reference experiment is described by a n -partite state $|\psi\rangle$ on Hilbert space $\mathcal{X} = \mathcal{X}_1 \otimes \dots \mathcal{X}_n$ and local measurement observables M_m for various m . Further, consider a physical experiment described by a n -partite state $|\psi'\rangle$ on Hilbert space $\mathcal{Y} = \mathcal{Y}_1 \otimes \dots \otimes \mathcal{Y}_n$ and local measurement observables M'_m for various m . We say that the physical experiment is equivalent⁴ to the reference experiment (and the physical state and measurement observables are equivalent to the reference state and measurement observables) if there exists a local isometry*

$$\Phi = \Phi_1 \otimes \dots \Phi_n, \quad \Phi_j : \mathcal{Y}_j \mapsto \mathcal{Y}_j \otimes \mathcal{X}_j \quad (3)$$

such that

$$\Phi(|\psi'\rangle) = |junk\rangle_{\mathcal{Y}} \otimes |\psi\rangle_{\mathcal{X}} \quad (4)$$

$$\Phi(M'_m |\psi'\rangle) = |junk\rangle_{\mathcal{Y}} \otimes M_m |\psi\rangle_{\mathcal{X}}. \quad (5)$$

The isometry Φ may be constructed by attaching ancillae in some product state $|00\dots 0\rangle_{\mathcal{X}}$ and applying local unitaries to the subsystems. Note that if we make any finite number of changes from the list above then we may construct a suitable local isometry and show that the experiment is equivalent to the reference experiment. Also, any experiment that is equivalent to the reference experiment may be constructed by applying changes from the list above: one simply attaches ancillae in the state $|junk\rangle$ and performs a suitable change of basis. The content of the main theorem is that, for a carefully chosen experiment, these are the *only* changes that preserve the statistics.

Theorem 1 (Mayers and Yao). *Suppose a physical experiment reproduces the statistics of the reference experiment described in section 3.2. Then the physical experiment is equivalent to the reference experiment.*

A simplified proof for the Mayers-Yao self-test is give in appendix C.

⁴ Note that this is not an equivalence relation since it is not symmetric.

3.2 Mayers-Yao self-test reference experiment

A general schematic for the Mayers-Yao reference experiment is shown in figure 1. A bipartite state $|\psi\rangle$ is distributed to a pair of measurement devices. The two measurement devices take classical inputs a and b , which each take one of three values. The devices then output classical bits, x and y .

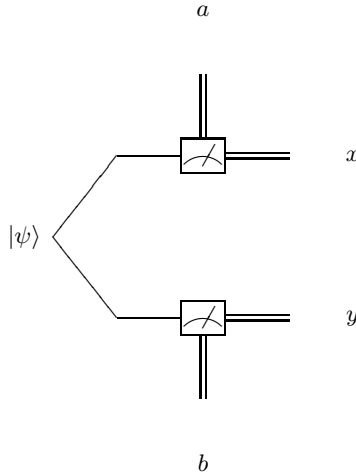


Fig. 1. Mayers-Yao self-test circuit

The reference state is an EPR pair $|\phi_+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and the reference measurement observables are $X, Z, \frac{X+Z}{\sqrt{2}}$ for each side of the EPR pair. For brevity we label $\frac{X+Z}{\sqrt{2}} = D$. For the untrusted physical devices this equality is not given, so there the separate label \tilde{D} is required.

4 Extending the Mayers and Yao self-test

The original Mayers and Yao EPR test utilized only a small set of measurements. Conspicuously missing is anything with complex coefficients. An important consequence of this is that the circuit test developed by Magniez et al. [MMMO06] is not able to test gates with complex coefficients; only gates with real coefficients can be tested. More specifically, real measurements reveal no information about the imaginary component of a density matrix.

In fact the Mayers-Yao self-test cannot be directly extended to include any measurements with complex coefficients. This is a result of the notion of equivalence used. Suppose that we wish to include the Y measurement in the set of reference measurements. The devices could instead implement $-Y$, the complex conjugate. So long as all complex measurements were complex conjugated it would be impossible to detect this change. Although this does not present an immediate problem - such a transformation is internally consistent and produces the correct outcome statistics - we cannot transform such a circuit back into the reference circuit using unitary transformations.

If this were the whole story we could simply require that the physical circuit be transformable into either the reference circuit or its complex conjugate. However, the real simulation, and now the general family of simulations, are also indistinguishable from the reference circuit and not unitarily transformable into the reference circuit.

We have one encouraging fact: all of the known simulations are equivalent to a simulation from the general family of simulations. We now prove that we can extend the Mayers-Yao test such that

these are the only simulations. Hence we may extend our notion of equivalence to include these simulations and obtain a new self-testing theorem.

Theorem 2. *Suppose a physical experiment duplicates the statistics generated by the reference experiment described in section 4.1. Then the physical experiment is equivalent to one of the simulations of the reference experiment described in section 2.*

4.1 Extended Mayers-Yao self-test reference experiment

The extended Mayers-Yao test will consist of three regular Mayers-Yao tests, performed together. Alice and Bob will perform the Mayers-Yao test with measurement settings (labelled with subscript A when used by Alice, and subscript B when used by Bob):

1. X , Z , and D
2. X , Y , and E
3. Y , Z , and F .

In the reference experiment the measurement settings X , Y and Z are realized by the Pauli operators, with $Y_B = -Y$ and otherwise $X_A = X_B = X$, $Y_A = Y$, $Z_A = Z_B = Z$. The other settings are realized by $D_A = \frac{X+Z}{\sqrt{2}}$, $E_A = \frac{X+Y}{\sqrt{2}}$, $F_A = \frac{Y+Z}{\sqrt{2}}$ on Alice's side and $D_B = \frac{X+Z}{\sqrt{2}}$, $E_B = \frac{X-Y}{\sqrt{2}}$, $F_B = \frac{Z-Y}{\sqrt{2}}$ on Bob's side. Bob's Y_B measurements all carry the -1 phase since measuring the state $|\phi_+\rangle$ with the operator $Y \otimes Y$ produces -1 instead of 1 as in the Mayers-Yao reference experiment. The reference state is again $|\phi_+\rangle$.

4.2 Proof of Theorem 2

We start by assuming that the states are all pure as in the Mayers-Yao test. Again we may incorporate the purification of a mixed state into either Alice or Bob's state by adding an ancilla.

First we apply the Mayers-Yao result with the measurements X , Z and D . We find a local isometry Φ as in definition 1. We extend Φ by adding an extra qubit for each side initialized in the state $|0\rangle$. Then Φ takes the X_A , Z_A , X_B and Z_B measurements to $X_{Q_A} \otimes I_{R_A} \otimes I_{S_A}$, $Z_{Q_B} \otimes I_{R_A} \otimes I_{S_A}$, $X_{Q_B} \otimes I_{R_B} \otimes I_{S_B}$ and $Z_{Q_B} \otimes I_{R_B} \otimes I_{S_B}$ where R_A and R_B are the added qubit registers and S_A and S_B are the junk registers. Meanwhile the state has the form $|\phi_+\rangle_{Q_A Q_B} \otimes |00\rangle_{R_A R_B} \otimes |junk\rangle_{S_A S_B}$.

We now consider the remaining measurements. The reference experiments for these measurements can be transformed using local unitaries into the usual Mayers-Yao reference experiments. Thus we may apply the result. However, we stop short of using the full result. Within the proof of Theorem 1 we achieve the following result.

Lemma 1. *Suppose a physical experiment reproduces the statistics of the Mayers-Yao reference experiment described in section 3.2. Then the physical measurements X_A and Z_A anti-commute on the support of the physical state, as do X_B and Z_B .*

This is shown in section C.2. When we apply this result to the remaining measurements in the extended test, we find that X_A and Y_A anti-commute on the support of the state, as do X_B and Y_B , Z_A and Y_A and Z_B and Y_B . For the remaining discussion we will limit ourselves to the support of the state.

Consider the A side measurements first. We may express Y_A as

$$Y_A = \sum_{P,E} y_{P,E} P_{Q_A} \otimes I_{R_A} \otimes E_{S_A}$$

where the P ranges over the Pauli operators and the E ranges over a basis for the Hermitian operators on S_A .

Since Y_A anti-commutes with $X_{Q_A} \otimes I_{R_A S_A}$ the coefficients of all the terms with $P = X$ must be 0. Indeed, since $-Y_A = (X_{Q_A} \otimes I_{R_A S_A}) Y_A (X_{Q_A} \otimes I_{R_A S_A})$ we have

$$-\sum_{P,E} y_{P,E} P_{Q_A} \otimes I_{R_A} \otimes E_{S_A} = \sum_{P \in \{I,X\}, E} y_{P,E} P_{Q_A} \otimes I_{R_A} \otimes E_{S_A} - \sum_{P \in \{Y,Z\}, E} y_{P,E} P_{Q_A} \otimes I_{R_A} \otimes E_{S_A}$$

where on the right hand side we have separated out the terms that commute with $X_{Q_A} \otimes I_{R_A S_A}$ and those that anti-commute. We see that we must have $y_{X,E} = -y_{X,E} = 0$ and $y_{I,E} = -y_{I,E} = 0$ for all E .

Applying similar reasoning and the test with Y and Z we find that $y_{Z,E} = 0$ for all E . Thus $Y_A = Y_{Q_A} \otimes I_{R_A} \otimes M_{S_A}$ for some Hermitian and unitary M_{S_A} . Next we compose Φ with a “phase kickback” circuit consisting of a Hadamard gate on the R_A register, followed by a controlled M_{S_A} , controlled on the R_A register, and a final Hadamard gate on the R_A register. This results in a new isometry (we will still call it Φ) such that

$$\Phi(Y_{Q_A} \otimes M_{S_A} |\psi\rangle) = Y_{Q_A} \otimes Z_{R_A} |\phi_+\rangle_Q |junk\rangle_{RS}. \quad (6)$$

This is essentially the well known translation of a two outcome measurement into a qubit measurement. Also, since the addition of the phase kickback did not operate on the junk register the X and Z measurements are not affected.

The above process can be repeated for Bob’s side, with analogous conclusions. In order to be consistent with the reference experiment, we may construct our isomorphism so that

$$\Phi(Y_{Q_B} \otimes M_{S_B} |\psi\rangle) = Y_{Q_B} \otimes Z_{R_B} |\phi_+\rangle_Q |junk\rangle_{RS}. \quad (7)$$

We have thus shown that the measurements are as in the general simulation.

We now turn our attention to the state. From the Mayers-Yao test on X and Z we know that the state on $Q_A \otimes Q_B$ (after applying Φ) is $|\phi_+\rangle$. We next consider the state on the remaining registers, $|junk\rangle_{RS}$. We may express this in the singular value (Schmidt) decomposition, split between R_{AB} and S_{AB} :

$$|\theta\rangle = \sum_j \lambda_j |j\rangle_{R_{AB}} |j\rangle_{S_{AB}} \quad (8)$$

with $\lambda_j > 0$. Since the Y measurement setting gives correlated results (recall we introduced a -1 factor on the B side measurement observable) and the form of Y_A and Y_B , the states $|j\rangle_{R_{AB}}$ must all be +1 eigenvectors of $Z_{R_A} \otimes Z_{R_B}$. If this were not the case then a -1 phase would be introduced and the measurement results would be incorrect at least some of the time. Thus the only possible states for $|j\rangle_{R_{AB}}$ are superpositions of $|00\rangle$ and $|11\rangle$. We do some relabelling and arrive at

$$|\psi\rangle = |\phi_+\rangle_{Q_{AB}} \otimes \left(\alpha |00\rangle_{R_{AB}} |\theta_{00}\rangle_{S_{AB}} + \beta |11\rangle_{R_{AB}} |\theta_{11}\rangle_{S_{AB}} \right) \quad (9)$$

with $|\theta_{00}\rangle$ and $|\theta_{11}\rangle$ not necessarily orthogonal. Note that tracing out the S_{AB} ancillae results in a state exactly as described by the multi-party simulation in section 2. Thus we have demonstrated that the physical experiment is equivalent to one of the general simulations of the reference experiment, and completed the proof of Theorem 2.

5 Cryptographic setting

Suppose that two or more parties are engaged in a cryptographic protocol using self-tested apparatus. The extended Mayers-Yao test above allows them to determine that the devices are implementing a simulation from the family of simulations described in section 2. Suppose further that the adversary, Eve, knows how the devices are implemented and controls the preparation of the state. The honest parties only perform operations as specified for the simulation. Eve, on the other hand, is free to interact with the extra qubits in the simulation in any way she likes. Does this give any advantage to Eve?

Eve can potentially perform many operations, including entangling a qubit of her own with the extra simulation qubits allowing her to perform simulation operations. She may also interact in complex ways with the extra simulation qubits along with the original register. Despite this, we are able to prove that Eve can gain no advantage for some protocols.

We explore a restricted class of protocols that are especially easy to analyse. These are protocols where the only operation that an honest party will do is a Pauli measurement. This class includes the six-state quantum key distribution protocol (implemented in as an entanglement based protocol) [BBBW84], [Bru98]. We will demonstrate that these protocols do not leak any more information when implemented using one of the simulations.

The proof is a series of security reductions to protocols in which each reduction only increases Eve's power. We will show that the final protocol in the reduction is just as secure as the reference protocol (without the simulation applied), hence the simulation protocol is also just as secure as the reference protocol.

For the first reduction we suppose that the participants in the protocol measure their simulation qubit in the Z eigenbasis after the protocol is completed, and transmit the result to Eve. This does not interfere with the intended protocol and only increases Eve's information. Since the Z measurement commutes with all simulation operations, the participants could just as well have performed the measurement before the protocol began. If Eve is the one who prepares the initial state for the simulation (in other cases Eve has strictly less power) then Eve could also perform this measurement herself. This measurement would collapse the state to an eigenvector of the Z measurements and Eve's strategy would be a mixture of different strategies with the states each an eigenvector of the Z measurements.

Let us examine the result of Eve choosing one of these eigenvector states. Each of the parties will receive their extra qubit prepared in a Z eigenvector. The effect of this on their operations is either to perform the protocol's original operation (in the case of a $|0\rangle$) or the complex conjugate (in the case of a $|1\rangle$.) For Pauli measurements, only the Y measurement is affected: the output bit is flipped in the case of the complex conjugate.

If every party receives the same eigenvector in their extra qubit, then the protocol reduces to either the original or the complex conjugate. In either case the security is identical to the original protocol. If the extra qubits are not in the same eigenvector then some Y measurements outcomes will be flipped and some will not. This does not affect Eve's information since she controls which outcomes are flipped and can undo the flips in her reckoning of the final classical information. Note that the bit flips may introduce errors into the protocol. If the protocol does not explicitly check for such errors (as does the 6-state protocol) information will still not be leaked to Eve, however a test for these errors may be required to make sure the protocol functions correctly. The final protocol, and hence the simulation, is thus as secure as the original protocol.

6 Conclusions and Future work

6.1 Conclusions

Theorem 2, along with the security result of section 5, allows us to analyze the case of the 6-state QKD protocol in the self-tested framework. In particular we may define a self-testing version of the 6-state protocol in which the extended Mayers-Yao test is incorporated along with the usual 6-state protocol. Given a robust version of the test (see section 6.2) we may first estimate the state and measurement observables, then apply a security proof for the 6-state protocol in order to derive a secure key rate.

Although a self-tested 6-state protocol is currently not practical, nor likely to become so, the result is interesting from a theoretical perspective within the self-tested framework. Previous results were limited to real Hilbert spaces, one could apply the real simulation explicitly within the reference experiment and then proceed with the self-test. This works fine for circuits, where only the correct outcome is important, however the 6-state protocol introduces other concerns, namely the possibility of information leaking to an adversary. The current work thus illustrates how a self-test for complex operations provides additional benefit over the previous self-tests.

6.2 Future work

Note that we have not described a physically realizable test in section 4. The proof requires that the expected value of the observables match the reference exactly. This cannot be established physically without some kind of repeatability assumptions and an infinite number of trials. The original test by Mayers and Yao was shown to be robust in [MMMO06], establishing a polynomial relationship between the precision of the statistics and the closeness to an EPR state. We are currently studying the robustness of these new tests. This is an important line of future research. A related task is to extend the results to continuous variable systems.

Another interesting line of research is to follow the same path as Magniez et al. to obtain a self-testing circuit for arbitrary circuits, now allowing complex gates. The framework and proofs from [MMMO06] offer a roadmap for such research, but there are some technical problems that arise along the way so a straightforward adaptation is not possible. These are due to the larger Hilbert space created when adding the extra qubits to allow the simulations.

Acknowledgements This work is supported by Canada’s NSERC, QuantumWorks, Ontario Centres of Excellence, MITACS, CIFAR, CRC, ORF, the Government of Canada, and Ontario-MRI.

References

- BBBW84. C. H. Bennett, G. Brassard, S. Breidbart, and S. Wiesner. Eavesdrop-detecting quantum communications channel. *IBM Technical Disclosure Bulletin*, **26**(8):4363 – 4366, January 1984.
- Bru98. Dagmar Bruß. Optimal eavesdropping in quantum cryptography with six states. *Phys. Rev. Lett.*, **81**(14):3018–3021, Oct 1998. DOI:10.1103/PhysRevLett.81.3018.
- Gis07. Nicolas Gisin. Bell inequalities: many questions, a few answers, 2007. EPRINT arXiv:quant-ph/0702021v2.
- MMG09. Matthew McKague, Michele Mosca, and Nicolas Gisin. Simulating quantum systems using real Hilbert spaces. *Physical Review Letters*, **102**(2):020505, 2009. DOI:10.1103/PhysRevLett.102.020505. EPRINT arXiv:0810.1923, URL <http://link.aps.org/abstract/PRL/v102/e020505>.
- MMMO06. Frédéric Magniez, Dominic Mayers, Michele Mosca, and Harold Ollivier. Self-testing of quantum circuits. In M et al. Bugliesi, editor, *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming*, number 4052 in Lecture Notes in Computer Science, pp. 72–83, 2006. EPRINT arXiv:quant-ph/0512111v1 .

- MY98. Dominic Mayers and Andrew Yao. Quantum cryptography with imperfect apparatus. In *FOCS*, pp. 503–509, September 1998. EPRINT arXiv:quant-ph/9809039.
- MY04. Dominic Mayers and Andrew Yao. Self testing quantum apparatus. *QIC*, 4(4):273–286, July 2004. EPRINT arXiv:quant-ph/0307205.
- vMMS00. Wim van Dam, Frederic Magniez, Michele Mosca, and Miklos Santha. Self-testing of universal and fault-tolerant sets of quantum gates. In *STOC '00: Proceedings of the thirty-second annual ACM symposium on Theory of computing*, pp. 688–696, New York, NY, USA, 2000. ACM. DOI:doi:10.1145/335305.335402. EPRINT arXiv:quant-ph/9904108 .

A Evolution in simulations

We can extend the measurement operator defined in 2 to arbitrary operators. We define

$$C(M) = |0\rangle\langle 0| \otimes M + |1\rangle\langle 1| \otimes M^*. \quad (10)$$

Note that $C(M)$ can be expressed differently as

$$C(M) = I \otimes \text{Re}(M) + iZ \otimes \text{Im}(M) \quad (11)$$

where $\text{Re}(M)$ and $\text{Im}(M)$ are the real and imaginary parts of M (both real matrices). In the case of a multi-party simulation, the Z operates on a particular party's added qubit.

We summarize some of the properties of $C(M)$ here

Lemma 2. *Let M and N be matrices. Then we have the following:*

1. $C(MN) = C(M)C(N)$.
2. $C(M + N) = C(M) + C(N)$.
3. Let a be a real number, then $C(aM) = aC(M)$.
4. If $|\psi\rangle$ is an eigenvector of M with eigenvalue λ , then $|0\rangle|\psi\rangle$ and $|1\rangle|\psi\rangle$ are eigenvectors of $C(M)$ with eigenvalues λ and λ^* , respectively.
5. $C(M)$ is Hermitian if and only if M is.
6. $C(M)$ is unitary if and only if M is.
7. $C(M)$ is positive semi-definite if and only if M is.
8. When M is Hermitian, $\text{Tr}(C(M)) = 2\text{Tr}(M)$.

These properties can be derived easily.

Discrete time evolution The properties of $C(\cdot)$ allow us to easily determine how the simulation states in the continuum evolve. Let U and $|\psi\rangle$ be a reference unitary operation and state and let ρ' be as in equation 1. By the form of $C(U)$ we have

$$\begin{aligned} C(U)\rho'C(U)^\dagger &= a|0\rangle\langle 0| \otimes U|\psi\rangle\langle\psi|U^\dagger + (1-a)|1\rangle\langle 1| \otimes U^*|\psi^*\rangle\langle\psi^*|U^T + \\ &\quad c|0\rangle\langle 1| \otimes U|\psi\rangle\langle\psi^*|U^T + c^*|1\rangle\langle 0| \otimes U^*|\psi^*\rangle\langle\psi|U^\dagger. \end{aligned}$$

But this is the simulation state for $U|\psi\rangle$, and hence $C(U)$ evolves the simulation state ρ' to produce a new simulation state corresponding to $U|\psi\rangle$. Compositions of unitaries will also evolve the state correctly so that the measurement statistics at the end of a circuit will be identical to that of the reference circuit.

General quantum operations may be mapped similarly. It is easy to verify that in Kraus representation a completely positive map is mapped to a completely positive map if we apply $C(\cdot)$ to each of the Kraus operators. The trace preserving property is also preserved. We apply the same reasoning as for U above to with each Kraus operator. The linearity of C then allows us to conclude that the simulation map will behave correctly. That is to say, it will map ρ' to a new simulation state corresponding to $|\psi\rangle$ evolved under the reference map.

Continuous time evolution We begin with a Hamiltonian H . One can simulate the Schrödinger evolution of H on $|\psi\rangle$ by evolving H^* on $|\psi^*\rangle$ backwards in time, or equivalently, evolving the system according to $-H^*$, and measuring with conjugated observables.

Thus, the simulation of the evolution of H can be achieved using the Hamiltonian

$$H' = |0\rangle\langle 0| \otimes H - |1\rangle\langle 1| \otimes H^*. \quad (12)$$

The evolution of the state according to the Schrödinger equation

$$U(t) = e^{-iH't} \quad (13)$$

gives

$$e^{-iH't} = |0\rangle\langle 0| \otimes e^{-iHt} + |1\rangle\langle 1| \otimes e^{-i(-H^*)t} = |0\rangle\langle 0| \otimes e^{-iHt} + |1\rangle\langle 1| \otimes (e^{-iHt})^* = C(e^{-iHt}) \quad (14)$$

(using the fact that $\exp(A+B) = \exp(A)\exp(B)$ when $AB=0=BA$, and that $\exp(P \otimes A) = P \otimes \exp(A)$ when $P^2=P$). Thus

$$e^{-iH't} = C(e^{-iHt}) \quad (15)$$

and the simulation evolution tracks that of the reference system.

Another way to arrive at the same H' is the approach used in the real simulation [MMG09]. There, rather than considering the Hamiltonian alone, the whole matrix in the exponent, $-iHt$, was considered. Applying $C(\cdot)$ to this matrix we obtain

$$|0\rangle\langle 0| \otimes (-iHt) + |1\rangle\langle 1| \otimes (-iHt)^* = i(|0\rangle\langle 0| \otimes H - |1\rangle\langle 1| \otimes H^*)t \quad (16)$$

Here the fact that $a^*b^* = (ab)^*$ means $(-iH)^* = iH^*$ and the -1 factor is explained.

B Real simulation in the family

The real simulation presented in [MMG09] can be expressed as a simulation in the family defined above through a change of basis. Starting with the state defined as in 1 with $a = c = \frac{1}{2}$ the simulation state is pure and equal to

$$|\psi'\rangle = \frac{1}{\sqrt{2}}|0\rangle|\psi\rangle + \frac{1}{\sqrt{2}}|1\rangle|\psi^*\rangle.$$

We next apply a Hadamard gate followed by the relative phase rotation

$$\begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix}$$

to the extra qubit. This is the same as applying the unitary

$$U = \begin{pmatrix} 1 & 1 \\ -i & i \end{pmatrix}. \quad (17)$$

The resulting state is

$$\frac{1}{2}|0\rangle(|\psi\rangle + |\psi^*\rangle) - \frac{i}{2}|1\rangle(|\psi\rangle - |\psi^*\rangle)$$

which can be rewritten as

$$|0\rangle \operatorname{Re}(|\psi\rangle) + |1\rangle \operatorname{Im}(|\psi\rangle)$$

which is the real simulation described in [MMG09]⁵.

Operators are transformed quite easily. For operator M we conjugate $C(M)$ by $U \otimes I$. From 11 we see that the resulting operator is

$$(U \otimes I)C(M)(U^\dagger \otimes I) = I \otimes \text{Re}(M) + XZ \otimes \text{Im}(M) \quad (18)$$

which is exactly the operator used in the real simulation for M .

The states used in the multi-party simulation in [MMG09] are stabilized by $Y_s \otimes Y_t$ for distinct s, t . Also note that the states used in the simulations defined here are stabilized by $Z_s \otimes Z_t$ for distinct s, t . The qubit-wise transformation applied transformations Z into Y , so the multi-party states are also transformed correctly.

C Simplified proof for Mayers-Yao self-test

C.1 Proof Overview

The main advantages of the following new proof for the Mayers-Yao self-test is that it is shorter, clearer, and more naturally extends to the more general test given in this paper.

The proof has two distinct parts. The first part establishes some equations on the state and observables based on the observed statistics. These are straightforward and are a direct result of the statistics observed. Next we use these equations to show that the X and Z observables on each side anti-commute on the support of the state. The second part uses the anti-commuting observables to construct local isometries that take the state and observables to the reference state and observables.

One important consideration is that of the support of the state. Since we do not make any claims about the state and observables outside the support of the state we disregard the rest of the Hilbert space. In this way we will not make any more reference to the support of the state.

C.2 Observed statistics imply anti-commuting observables

Statistics In the reference test the marginals for each observable are all 0. That is,

$$\langle \phi_+ | M \otimes I | \phi_+ \rangle = 0$$

for $M \in \{X, Z, D\}$. (Swapping the systems in this and the following equations gives the same result since $|\phi_+\rangle$ is symmetric.) Measuring the same observable on both sides always give identical outcomes. Thus

$$\langle \phi_+ | M \otimes M | \phi_+ \rangle = 1.$$

Additionally, X and Z measurements are uncorrelated.

$$\langle \phi_+ | X \otimes Z | \phi_+ \rangle = 0.$$

The interesting part comes when we measure X or Z on one side and D on the other.

$$\langle \phi_+ | X \otimes D | \phi_+ \rangle = \langle \phi_+ | Z \otimes D | \phi_+ \rangle = \frac{1}{\sqrt{2}}.$$

⁵ This part of the real simulation was previously well known

State equalities Using the equations from section 3.2 on the measurement outcomes combined with the fact that $|\psi\rangle$ is normalized gives us the following equations

$$|\psi\rangle = X_A \otimes X_B |\psi\rangle \quad (19)$$

$$= Z_A \otimes Z_B |\psi\rangle \quad (20)$$

$$= D_A \otimes D_B |\psi\rangle \quad (21)$$

$$X_A \otimes I |\psi\rangle = I \otimes X_B |\psi\rangle \quad (22)$$

$$Z_A \otimes I |\psi\rangle = I \otimes Z_B |\psi\rangle \quad (23)$$

$$D_A \otimes I |\psi\rangle = I \otimes D_B |\psi\rangle \quad (24)$$

$$X_A Z_A \otimes I |\psi\rangle = I \otimes Z_B X_B |\psi\rangle \quad (25)$$

$$Z_A X_A \otimes I |\psi\rangle = I \otimes X_B Z_B |\psi\rangle \quad (26)$$

$$X_A Z_A \otimes I |\psi\rangle = X_A \otimes Z_B |\psi\rangle \quad (27)$$

$$Z_A X_A \otimes I |\psi\rangle = Z_A \otimes X_B |\psi\rangle \quad (28)$$

We can also establish some orthogonality relationships between various vectors. In particular the vectors $|\psi\rangle, X_A \otimes I |\psi\rangle, Z_A \otimes I |\psi\rangle, X_A Z_A \otimes I |\psi\rangle$ are pairwise orthogonal.

Our goal for the remainder of the proof is to show that any state for which these equations hold must be equivalent to $|\phi_+\rangle$.

Anti-commuting observables We now move to more salient matters. First, we note that $D_A \otimes I |\psi\rangle$ must be in the space spanned by $X_A \otimes I |\psi\rangle$ and $Z_A \otimes I |\psi\rangle$ because it has overlap $\frac{1}{\sqrt{2}}$ with each of these orthogonal vectors, and it has norm 1. Thus

$$D_A \otimes I |\psi\rangle = \frac{X_A + Z_A}{\sqrt{2}} \otimes I |\psi\rangle$$

and analogously for $I \otimes D_B |\psi\rangle$. This allows us to make the following deductions

$$\begin{aligned} |\psi\rangle &= D_A \otimes D_B |\psi\rangle \\ &= \frac{1}{2} (X_A + Z_A) \otimes (X_B + Z_B) |\psi\rangle \\ &= |\psi\rangle + (X_A \otimes Z_B + Z_A \otimes X_B) |\psi\rangle \end{aligned}$$

Applying equations 22 and 23 we obtain

$$(X_A Z_A + Z_A X_A) \otimes I |\psi\rangle = 0. \quad (29)$$

By Lemma 3, below, it follows that X_A and Z_A anti-commute on the support of $|\psi\rangle$ on A . Similarly, the observables X_B and Z_B anti-commute on support of $|\psi\rangle$ on B .

Lemma 3. *Let X_A and Z_A be operators and $|\psi\rangle_{AB}$ a bipartite state such that*

$$X_A Z_A \otimes I_B |\psi\rangle_{AB} = -Z_A X_A \otimes I_B |\psi\rangle_{AB}. \quad (30)$$

then $X_A Z_A |\phi\rangle = -Z_A X_A |\phi\rangle$ for any $|\phi\rangle$ in the support of $|\psi\rangle_{AB}$ on A .

Proof. Let

$$|\psi\rangle = \sum_j \lambda_j |j\rangle_A |j\rangle_B. \quad (31)$$

be the singular value decomposition of $|\psi\rangle$. We then have

$$X_A Z_A \otimes I_B \sum_j \lambda_j |j\rangle_A |j\rangle_B = -Z_A X_A \otimes I_B \sum_j \lambda_j |j\rangle_A |j\rangle_B. \quad (32)$$

We now take the inner product with $|k\rangle_A |k'\rangle_B$ for some k, k' to obtain

$$\lambda_j \langle k|_A X_A Z_A |j\rangle_A = -\lambda_j \langle k|_A X_A Z_A |j\rangle_A \quad (33)$$

When we restrict to the subspace to the subspace spanned by the $|k\rangle_A$ for which $\lambda_k \neq 0$ (i.e. on the support of $|\psi\rangle$ on A) we find that $X_A Z_A = -Z_A X_A$.

C.3 Local unitary transformations

Now we can easily build the local unitaries required to extract the EPR pair. We use the circuit shown in figure 2. There the outer $|0\rangle$ states are added while the two inner wires carry the two halves of the bipartite state $|\psi\rangle$. This circuit essentially builds a SWAP gate out of two CNOT gates (the usual third gate is not necessary since we initialize with $|0\rangle$.) The SWAP gate extracts the entanglement out of $|\psi\rangle$ and swaps in a product state.

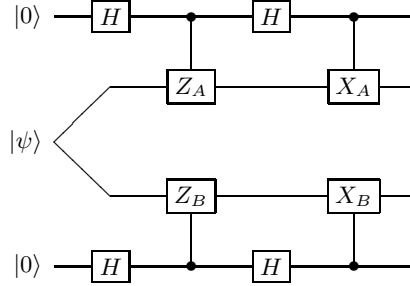


Fig. 2. Circuit for Φ showing equivalence of physical circuit to reference circuit in Mayers-Yao test

The circuit gives two isometries, one for each wire in EPR test circuit, which we denote Φ_A and Φ_B .

State After applying this circuit the resulting state is

$$\begin{aligned} \Phi_A \otimes \Phi_B(|\psi\rangle) &= \frac{1}{4}(I + Z_A) \otimes (I + Z_B) |\psi\rangle |00\rangle \\ &+ \frac{1}{4}(I + Z_A) \otimes X_B(I - Z_B) |\psi\rangle |01\rangle \\ &+ \frac{1}{4}X_A(I - Z_A) \otimes (I + Z_B) |\psi\rangle |10\rangle \\ &+ \frac{1}{4}X_A(I - Z_A) \otimes X_B(I - Z_B) |\psi\rangle |11\rangle \end{aligned}$$

Applying some equations and the anti-commuting result from the previous section we find that this is equal to

$$\begin{aligned}\Phi_A \otimes \Phi_B(|\psi\rangle) &= \frac{1}{4}(I + Z_A) \otimes (I + Z_B) |\psi\rangle (|00\rangle + |11\rangle) + \\ &(I + Z_A)(I - Z_A) \otimes X_B |\psi\rangle |01\rangle + X_A \otimes (I + Z_B)(I - Z_B) |\psi\rangle |10\rangle \\ &= \frac{1}{\sqrt{2}}(I \otimes I + I \otimes Z_B) |\psi\rangle |\phi_+\rangle\end{aligned}$$

This may look curious since $I + Z_A$ and $I + Z_B$ are not unitary. In fact it is easy to show that the final state still has the correct norm. To give some intuition, note that in the reference case we want to extract $|\phi_+\rangle$ and swap in $|00\rangle = \frac{1}{\sqrt{2}}(I + Z) \otimes (I + Z) |\phi_+\rangle$.

Measurement operators We now turn to equivalence of the measurement operators. We start with X_A (the result for X_B follows analogously). Applying X_A to $|\psi\rangle$ before applying the circuit is the same as applying it at the end, with a -1 phase introduced by anti-commuting past the controlled Z_A operation (recall from section C.2 that X_A and Z_A anti-commute on the relevant subspace). The resulting state is

$$\begin{aligned}\Phi_A \otimes \Phi_B(X_A \otimes I_B |\psi\rangle) &= \frac{1}{4}X_A(I - Z_A) \otimes (I + Z_B) |\psi\rangle |00\rangle \\ &+ \frac{1}{4}X_A(I - Z_A) \otimes X_B(I - Z_B) |\psi\rangle |01\rangle \\ &+ \frac{1}{4}(I + Z_A) \otimes (I + Z_B) |\psi\rangle |10\rangle \\ &+ \frac{1}{4}(I + Z_A) \otimes X_B(I - Z_B) |\psi\rangle |11\rangle\end{aligned}$$

Following the same logic as used in the state equivalence, we find that the final state is

$$\Phi_A \otimes \Phi_B(X_A \otimes I |\psi\rangle) = \frac{1}{\sqrt{2}}(I \otimes I + I \otimes Z_B) |\psi\rangle (X \otimes I) |\phi_+\rangle$$

For the Z_A operation, we see that the effect is a -1 phase kicked back through the final controlled X_A operation. This phase appears on the terms with $|1\rangle$ in the qubit, exactly as if a Z operation had been applied to the qubit. The equivalence for the D operators results from the fact that $D = \frac{X+Z}{\sqrt{2}}$ on the relevant subspace, and linearity.

This concludes the proof of Theorem 1 .